УДК 004.056.5 Вестник УрФО № 1(47) / 2023, с. 43–50

Акбулякова Л.М., Шабуров А.С.

DOI: 10.14529/secur230104

О СОВЕРШЕНСТВОВАНИИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ВЗАИМОДЕЙСТВИИ ОПЕРАТОРА С РЕГИОНАЛЬНЫМ СЕГМЕНТОМ «ЕГИС3»

В статье рассматривается решение по модернизации защиты информационной системы персональных данных, с целью устранения ее уязвимостей при информационном взаимодействии. Сформулирована проблема поиска оптимальных решений по обеспечению информационной безопасности при централизованной обработке данных. Определены наиболее уязвимые процессы действующей информационной системы персональных данных. Проанализированы применяемые методы и средства защиты информации, удовлетворяющие требованиям при взаимодействии с «ЕГИС3». Предложено решение по устранению выявленных уязвимостей на основе открытого программного обеспечения. Проведена оценка эффективности внедрения программного обеспечения на основе выбранных показателей эффективности.

Ключевые слова: *центр обработки данных, защита информации, информационная система персональных данных, демилиторизированная зона, показатель эффективности.*

ON IMPROVEMENT OF THE SYSTEM OF PROTECTION OF PER-SONAL DATA IN THE INTERACTION OF THE OPERATOR WITH THE REGIONAL SEGMENT «EGISZ»

The article discusses the decision to modernize the protection of the infor-mation system of personal data, in order to eliminate its vulnerabilities during in-formation interaction. The problem of finding optimal solutions to ensure infor-mation security in the case of centralized data processing is formulated. The most vulnerable processes of the current information system of personal data are deter-mined. The applied methods and means of information protection that meet the re-quirements when interacting with the EGISZ are analyzed. A solution is proposed to eliminate the identified vulnerabilities using Elastic Stack. An assessment of the ef-fectiveness of the implementation of information security tools was carried out by comparing performance indicators.

Keywords: *data processing center, information security, personal data infor-mation system, demilitarized zone, performance indicator.*

Повсеместное внедрение единых центров обработки данных (ЦОД) позволяет обеспечить качественно более совершенный набор сервисов информационного обеспечения, повысить оперативность информационного обмена, обеспечить множество иных преимуществ. Кроме того, подобные решения информационных систем предполагают внедрение новых, эффективных моделей и методов обеспечения информационной безопасности. В тоже время, способы проникновения вредоносной информации в подобные информационные системы также может модифицироваться, что предполагает поиска и применения как новых средств и методов защиты, так и оптимизации архитектуры информационных систем. Например, совершенствование архитектуры информационного взаимодействия оператора ИСПДн с Единой государственной информационной системой в сфере здравоохранения (ЕГИСЗ), позволяет повысить эффективность обеспечения защиты информации, при этом, обеспечивая выполнение заданных характеристик самой системы [1, 2]. В то же время, развитие процессов информационного взаимодействия требует поиска новых, более совершенных решений по защите информации. Это особенно важно в условиях роста количества и сложности кибератак, прекращения функционирования и ухода с российского рынка отдельных поставщиков информационных услуг, а также временных и финансовых ограничений.

При разработке средств, методов и мероприятий обеспечения информационной безопасности необходимо учитывать большое количество различных факторов: возможные источники угроз, уязвимости, ценность информации, которую необходимо защищать, техническая оснащенность объекта информатизации и т.д. В данной работе в качестве объекта защиты информации рассмотрена информационная система персональных данных (ИСПДн), предназначенная для обработки данных при взаимодействия оператора ИСПДн с ЕГИСЗ (рис. 1).

Цель исследования заключалась в поиске

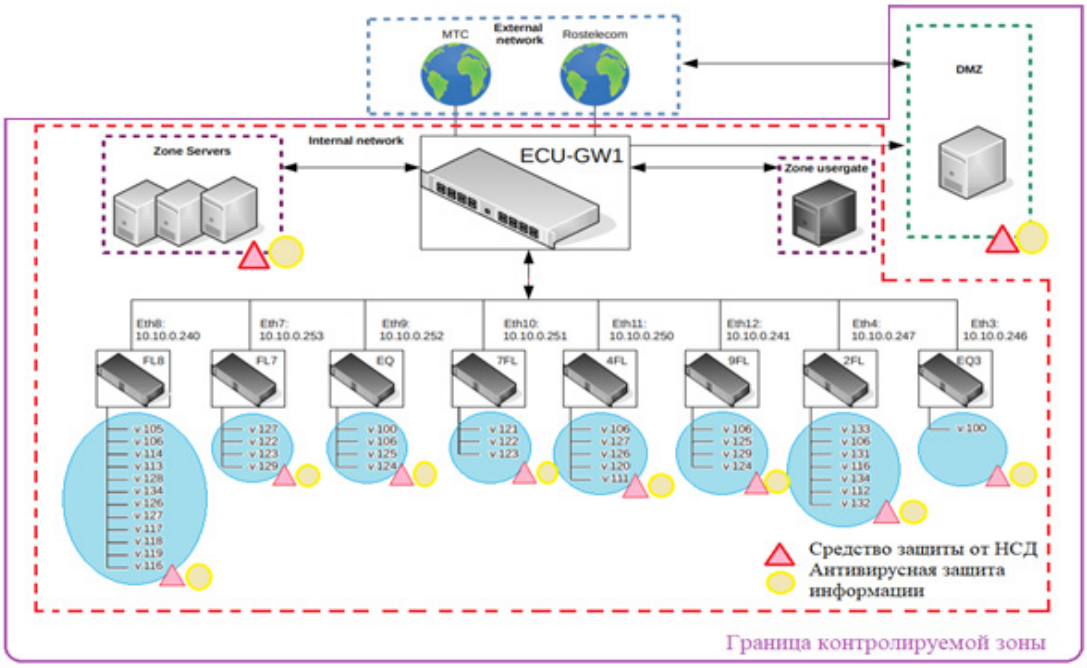

Рис. 1. Структурная схема оъекта защиты

оптимальных решений по обеспечению информационной безопасности ИСПДн, за счет определения характеристик внедренной системы защиты информации, установление взаимосвязей между ее характеристиками и показателями эффективности защиты в отдельных аспектах информауионной безпасности.

Особенностью реализованной структуры СЗИ является разделение защищаемой сети на несколько вланов, что позволяет логически ограничивать сетевое взаимодействие между автоматизированными рабочими местами (АРМ), выполняеющих различные функции. В структуре сети предусмотрена демилиторизированная зона (ДМЗ), в которой размещается веб-сервер объекта защиты, имеющий прямой и обратный доступ к внешней сети, но ограниченый по взаимодействию с внутренней сетью организации. Подобная конфигурация направлена на усиление безопасности внутренней сети организации, в которой открытые для общего доступа сервера находятся в отдельном изолированном сегменте. Данная концепция обеспечивает отсутствие контактов между открытыми для общего доступа серверами и другими сегментами сети в случае несанкционированного доступа к серверу.

Применение UserGate, как основного средства защиты инфмации, представляещего собой универсальный шлюз, объединяющий межсетевой экран, маршрутизацию, шлюзовой антивирус, систему обнаружения и предотвращения вторжений, систему фильтрации, модуль мониторинга и статистики и многие другие функции позволяет реализовать основные требования по обеспечению безопасности информации для ИСПДн [3]. Анализ функционирования данного средства ЗИ позволяет сделать вывод о достаточно эффективном управлении информационной безопасностью информационной системы, оптимизировать трафик информационного взаимодействия, и эффективно предотвращать основные угрозы безопасности информации.

В качестве средства защиты информации от несанкционированного доступа (НСД) применяется Secret Net Studio и технология ViPNet, как комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования. Программно-аппаратные средства позволяют эффективно блокировать неавторизованных пользователей, а технические средства предназначены для исключения физического проникновения посторонних субъектов в пределы контролируемой зоны [4].

Антивирусная защита организована на основе внедрения программного антивирусного средства Dr.Web, что обеспечивает выявление широкого спектра вредоносных

программ, восстановления поврежденных файлов, предохранение операционной системы или отдельных файлов от заражения.

Взаимодействие четырех сегментов сети необходимо осуществляется внутри контролируемой зоны объекта и обеспечивается средствами защиты от НСД, а также средствами антивирусной средство защиты информации. Детализированная схема взаимодействия сети на основе разделения на изолированные сегменты, с применением средств защиты информации представлена на рис. 2.

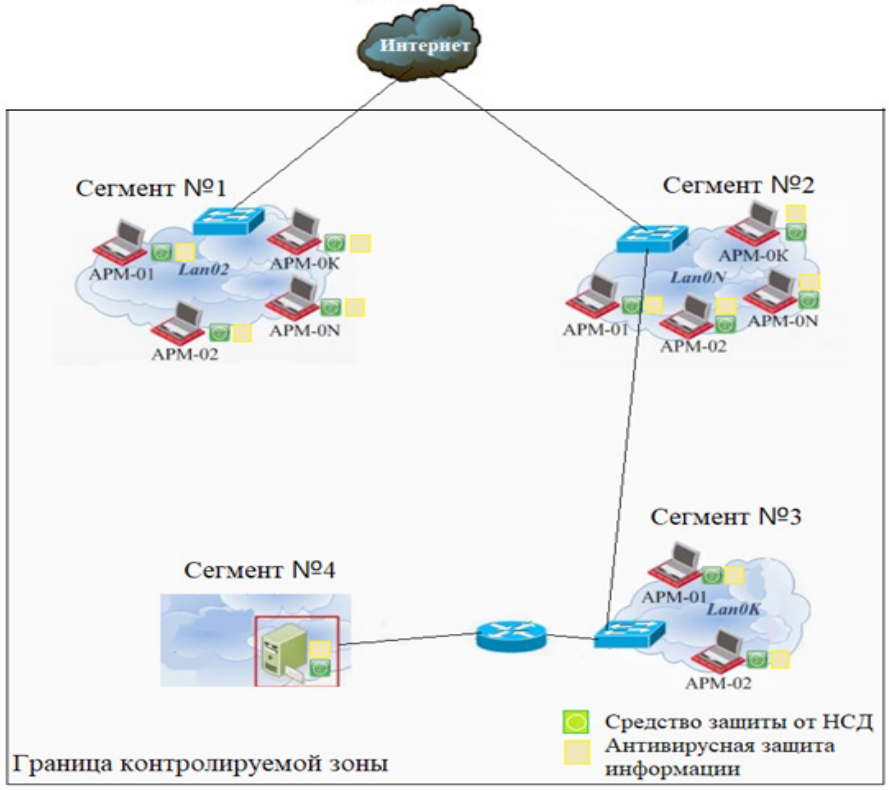

Рис. 2. Схема взаимодействия сегментов сети

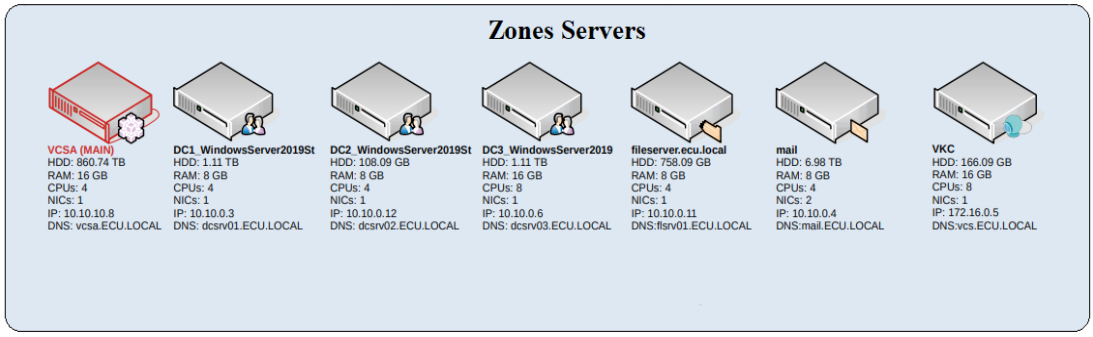

Рис. 3. Зона серверного оборудования объекта защиты

Функционирование объекта защиты осуществляется на основе специализированного серверного оборудования структурно объединенных в зону серверов (рис. 3).

В зону серверного оборудования входят семь серверных станций, выполняющих основные функции по обработке данных, такие как: контроль и создание учетных записей, хранение информации объекта информатизации, почтовое взаимодействие, организация физической защиты информации, а также взаимодействие по видеосвязи [5].

В процессе плановой эксплуатации ИСПДн была выявлена уязвимость сервера электронной почты Zimbra, работающего с использованием пакета программного обе-

спечения для совместной работы. Уязвимость заключалась в значительном количестве несанкционированных запросов, что в конечном итоге могло способствовать реализации угрозы типа «отказ в обслуживании».

Для предотвращения выявленной уязвимости было использовано программное обеспечение с открытым исходным кодом ElasticStack с помощью сервиса централизованного ведения журнала на основе Rsyslog. В частности, были установлены центральный сервер ведения журналов и эластичный стек, обновления. В этом журнале был настроен сервер RSyslog для принудительного использования TLS. Также были разработаны сертификаты TLS для сервера и клиента Rsyslog.

Для корректной работы сервера Rsyslog потребовалась его настройка, в соответствии с глобальными директивами. Данная конфигурация необходима для применения шифрования TLS и аутентификации в RSyslog и обеспечивает доступ на почтовый сервер только доверенных клиентов.

В целях визуализации оценки эффективности принятого решения было использовано программное обеспечение с открытым исходным кодом, позволившее провести анализ журналов и временных рядов, а также мониторинг приложений и текущих процессов.

Выбор необходимых компонентов программного обеспечения и их настроек позволил проанализировать несанкционированные попытки входа в информационную систему. Для этого с помощью журнала регистрации событий было выявлено, что за 1.5 минуты были осуществлены 3 несанкционированные попытки входа в систему через пользовательские учетные записи. На основе детального анализа логов были выделены соответствующие ip-адреса за экспериментальный промежуток времени. В результате эксперимента были выявлены несанкционированные попытки входа в систему со 190 посторонних ip-адресов. Подобная статистика не является критичной, но при определенных обстоятельствах может привести к перегрузке серверного оборудования из-за возрастания очереди запросов.

Рис. 4. Результат оценки несанкционированных попыток доступа

На рис. 5 представлено графическое представление результатов анализа логов несанкционированного входа в информационную систему.

Для оценки эффективности предлагаемого решения отслеживалось состояние всех процессов, происходящих на сервере. В качестве основных показателей эффективности обеспечения безопасного взаимодействия были выбраны:

1) t – промежуток времени, за которое происходят попытки входа в систему;

2) p – количество неуспешных попыток входа в систему;

3) i – количество ip-адресов, посредством которых происходят несанкционированные доступы в систему.

За экспериментальный период продолжительностью 7 дней были проведены контрольные оценки выбранных показателей

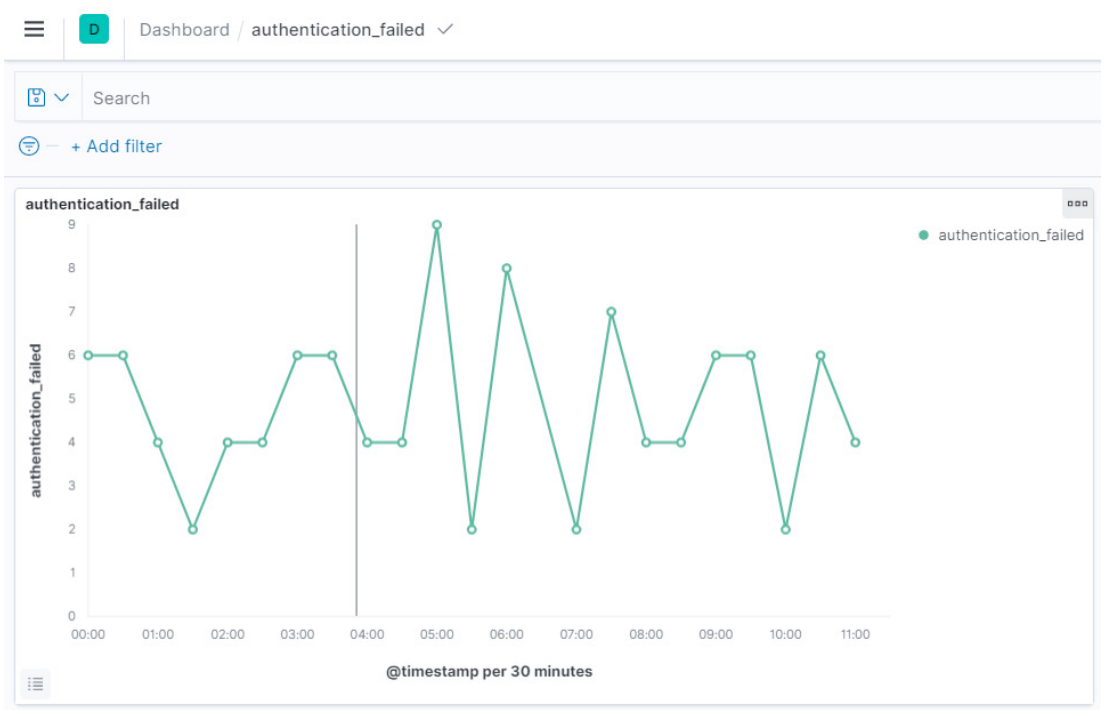

Рис. 5. Анализ логов несанкционированного входа в систему

эффективности без учета применения и с применением программного обеспечения ElasticStack. Результаты контрольных оценок представлены в таблицах 1–3.

Таблица 1

Значения показателя t

n	Значение t до внедрения (ч)	Значение t после внедрения (ч)
1	0,33	4,5
2	0,33	5,5
3	0,5	6,5
4	0,5	4,5
5	0,67	5,5
6	0,67	7,5
7	0,67	7,5

Таблица 2

Значения показателя p

n	Значение p до внедрения	Значение p после внедрения
1	193	6
2	205	5
3	217	4
4	208	6
5	211	5
6	220	3
7	231	3

Количественное сравнение неуспешных попыток входа в систему и ip-адресов, с помощью которых происходят несанкционированные входы в систему до и после внедрения ElasticStack за экспериментальный период представлен на рис. 6.

Таблица 3

Значения показателя i

n	Значение i до внедрения	Значение i после внедрения
1	190	5
2	200	4
3	215	4
4	207	5
5	210	4
6	220	3
7	230	3

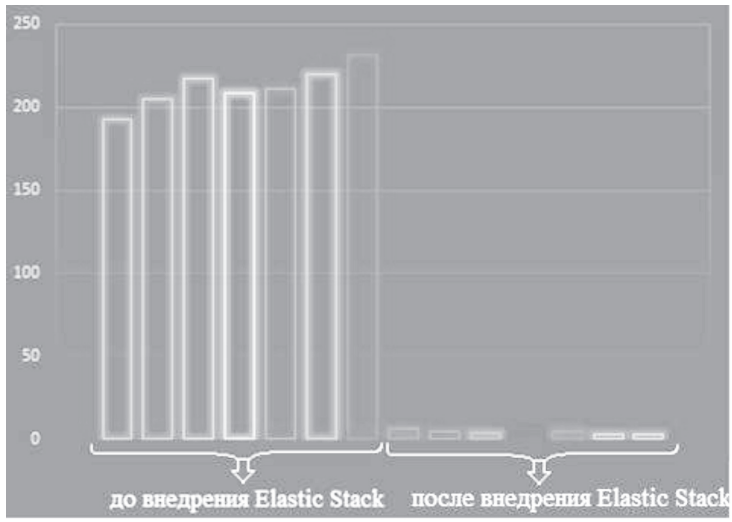

Рис. 6. Количественное сравнение неуспешных попыток входа в систему

Анализ полученных данных показывает, что после блокирования ip-адресов с помощью которых происходят попытки доступа, значительно уменьшается количество неуспешных попыток несанкционированного входа в информационную систему. В свою очередь, значение показателя t -промежуток времени, за которое происходят попытки входа в систему, наоборот возрастает, что также свидетельствует об уменьшении количества попыток несанкционированного доступа и эффективности предлагаемого решения.

Таким образом, на основе внедрения программного обеспечения ElasticStack была решена задача блокирования потенциально опасных ip-адресов, уменьшения нагрузки на серверное оборудование и всю информационную систему, что способствует уменьшению вероятности угроз безопасности информации в ИСПДн. Данное решение может являться временным, с учетом требований по импортозамещению. В то же время, в отдельных ситуациях подобные решения позволяют повышать эффективность обеспечения информационной безопасности за счет свободно распространяемого программного обеспечения, в сочетании с применением штатных методов и средств защиты информации, в том числе и при взаимодействии оператора ИСПДн с региональным сегментом ЕГИСЗ.

Литература

1. Акбулякова Л.М., Шабуров А.С. «О совершенствовании архитектуры информационной системы персональных данных при взаимодействии оператора с сегментом «ЕГИСЗ»// Вестник УрФО. Безопасность в информационной сфере. 2021. № 4(42). С 15–23.

2. Постановление правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения (ЕГИСЗ)»

3. Методические рекомендации медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках единой государственной информационной системы в сфере здравоохранения: официальный сайт. – Москва. – 2018. – URL: https://portal.egisz.rosminzdrav.ru (дата обращения 15.11.2022).

4. Решения по комплексному обеспечению информационной безопасности в ЕГИСЗ: официальный сайт. – Москва. – 2019. – URL: https://portal.egisz.rosminzdrav.ru (дата обращения 15.11.2022).

5. Техническое задание «Оказание услуги комплексного сервиса в целях обеспечения сервисной поддержки функционирования медицинской организации в рамках регионального сегмента единой государственной информационной системы в сфере здравоохранения»: официальный сайт. – Москва. - 2020. - URL: https://vkr.pspu.ru/uploads (дата обращения 20.11.2022).

References

1. Akbulyakova L.M., SHaburov A.S. «O sovershenstvovanii arhitektury informacionnoj sistemy personal'nyh dannyh pri vzaimodejstvii operatora s segmentom «EGISZ»// Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2021. № 4(42). S 15–23.

2. Postanovlenie pravitel'stva Rossijskoj Federacii ot 09.02.2022 № 140 «O edinoj gosudarstvennoj informacionnoj sisteme v sfere zdravoohrane-niya (EGISZ)»

3. Metodicheskie rekomendacii medicinskim organizaciyam po organizacii kriptograficheskoj zashchity kanalov pri vzaimodejstvii v ramkah edinoj gosudarstvennoj informacionnoj sistemy v sfere zdravoohraneniya: oficial'nyj sajt. – Moskva. – 2018. – URL: https://portal.egisz.rosminzdrav.ru (data obrashche-niya 15.11.2022).

4. Resheniya po kompleksnomu obespecheniyu informacionnoj bezopasnosti v EGISZ: oficial'nyj sajt. – Moskva. – 2019. – URL: https://portal.egisz.rosminzdrav.ru (data obrashcheniya 15.11.2022).

5. Tekhnicheskoe zadanie «Okazanie uslugi kompleksnogo servisa v celyah obespecheniya servisnoj podderzhki funkcionirovaniya medicinskoj organizacii v ramkah regional'nogo segmenta edinoj gosudarstvennoj informacionnoj sistemy v sfere zdravoohraneniya»:oficial'nyj sajt. – Moskva. – 2020. – URL: https://vkr.pspu.ru/uploads (data obrashcheniya 15.11.2021).

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент, доцент кафедры автоматики и телемеханики, Пермский национальный исследовательский политехнический университет. Россия, 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: shans@at.pstu.ru

АКБУЛЯКОВА Лилия Маратовна, студент, Пермский национальный исследовательский политехнический университет. Россия, 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: akbulyakowa@mail.ru

SHABUROV Andrey Sergeevich, Candidate of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. E-mail: shans@at.pstu.ru

AKBULYAKOVA Liliya Maratovna, student, Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Ave, 29. E-mail: akbulyakowa@mail.ru